State of Tennessee

Department of Finance and Administration
Office for Information Resources
Security Policy and Audit

Cyber Security Awareness Month Presentation
Information Security: At Home

Welcome (Slide 1)

Welcome to a short information security lesson, “Information Security: At Home.” This tutorial is brought to you by the State of Tennessee’s Security Management Group to promote Cyber Security Awareness Month.

Lesson Introduction (Slide 2)

This lesson will have four sections: protecting your kids online, security software, wireless networks and computer end-of-life. At the end of the lesson there is a resource page incase you would like additional information.

Section One: Protecting Your Kids Online (Slide 3)

It is up to you as a parent to decide where your kids can go online. There are some products to help you restrict access to websites you do not want your kids going to. Some internet service providers (ISPs) have parental controls that offer site blocking, restrict access to chat rooms, and other similar features. Also, there are other online services that can provide you with parental controls or web-content filtering to restrict access to websites.

Increasing the security and privacy settings on your computer can aid you in protecting your kids while they are online. As a parent you can create an administrator account to perform system administrator tasks such as loading new software. You can create multiple user accounts for your computer so that everyone can have access to the computer with their own Desktop and Documents folder. When you create the user accounts you should make them limited user accounts or restricted access accounts. This way you are limiting the access your kids have to your computer and you are preventing them from installing new hardware or software unless you, as the Administrator, install it for them. Also, you can adjust your web browser settings to assign security and privacy preferences to websites.

Educating your kids about online practices is the best way to protect them from online predators. You should teach and remind your kids about the dangers of talking to strangers online. Your kids should never give out any of their personal information online that includes their age, gender, location or address, phone number, first and last name, and e-mail address. Instead your kids should use their first name or a nickname while they are online. They should never agree to meet someone in person they met online without parental supervision. And they should never send pictures of themselves to people they do not know or that they met online.

Section Two: Security Software (Slide 4)

You should never assume your security software is protecting your computer simply because you have it installed on your computer. New viruses are created frequently, and software sometimes needs security updates. Also, incase of theft you want your computer to be protected by having your computer password protected by setting up a user account on your computer.

If you are not updating your computer regularly it can become vulnerable to attacks and viruses. Therefore, you should enable your computer’s automatic updating feature to receive updates for your operating system and software. However, if you are using dial-up for your Internet connection you should run your computer updates manually because it can take a long time to update your computer. Anti-virus software should be enabled to check for new signatures and run scheduled scans. Your firewall should always be turned on because it protects you from attackers that want to steal your information or harm your computer. Use a spyware solution to protect yourself from being tracked in an attempt to gain personal information about you. Spyware is also harmful to your computer because it can slow down your computer.

Section Three: Wireless Networks (Slide 5)

Securing your wireless network at home is important so that you are not giving away free Internet access to everyone within range of your network. If too many people are connected to your wireless network your connection might be slow, you could exceed the number of connections allowed by your Internet Service Provider (ISP), malicious users could use your wireless network to perform illegal activities, sensitive information could be stolen, or malicious programs could be installed on your computer. Therefore, you should secure your wireless network by changing various default settings on your wireless access point device.

Default passwords are used by manufactures, and when you receive your wireless access point device you should change the Administrative password as soon as possible. When you are creating a new Administrative password you should make it a long password that does not contain personal information (birth date, zip code, etc.), and it should have alpha, numeric and special characters. Another manufacturer default setting is for the wireless network name. Again, when you rename your wireless network you should pick something that is hard to guess.

Encrypting the wireless traffic from your wireless access device to your computer is another way to make your wireless network secure. When you setup your wireless network you should have an option to enable encryption. During the setup process you should look for “WPA” to turn on the encryption. If you have already setup your wireless access device you should check your settings to make sure encryption is enabled.

Two features should be disabled or turned off: remote administration and universal plug and play. Finally, if you have the ability to disable identifier broadcasting you should do so because this will make your wireless network somewhat invisible to others. Not all wireless access devices have this capability, you should check your owner’s manual to determine if you have this option or not.

Section Four: Computer End-of-Life (Slide 6)

One day you might decide your old computer needs to be replaced, or you just want to get the latest and greatest new model. No matter the reason, there are a few things you should be mindful of when getting rid of your old computer.

Consider the type of business you have conducted on your computer, and then think of the damage that could be done if someone obtained the information on your computer. Just because you delete a file on your computer does not mean it cannot be recovered until it is properly wiped from your hard drive. If you are selling, donating or disposing of your computer you should consider buying software to overwrite the disk. The process of overwriting your disk multiple times can be time consuming, but it is the most reliable method of wiping your hard drive clean of all your data. If you are only disposing of your computer physically destroying the hard drive is just as effective as wiping the hard drive clean.

There are many e-waste recycling programs for you to take advantage of when you are disposing of your old computer equipment. Many computer manufacturers and retailers have recycling programs for people to dispose of their outdated computer equipment; some will even pickup the old equipment at your home. Computer equipment includes the computer and its accessories such as printer, scanner, keyboard, modem, mouse, and monitor.

Conclusion (Slide 7)

Thank you for taking the time to learn about information security at home. Four recourses are available for additional information: US-CERT White Paper, Microsoft articles about increasing security and cleaning hard drives, and an article issued by CNN regarding safe online practices.